

# The Classification of Circulant Weighing Matrices of Weight 16 and Odd Order

R. M. Adin\*, L. Epstein and Y. Strassler

*E-mail:* radin, epstin and strasler (@macs.biu.ac.il)

Department of Mathematics and Computer Science

Bar-Ilan University

Ramat-Gan 52900, Israel

October 14, 1999

## Abstract

In this paper we completely classify the circulant weighing matrices of weight 16 and odd order. It turns out that the order must be an odd multiple of either 21 or 31. Up to equivalence, there are two distinct matrices in  $CW(31, 16)$ , one matrix in  $CW(21, 16)$  and another one in  $CW(63, 16)$  (not obtainable by Kronecker product from  $CW(21, 16)$ ). The classification uses a multiplier existence theorem.

## 1 Introduction

In the last decade we have witnessed an enormous amount of activity in the field of designs. One of the most active subfields is the subject of orthogonal designs. It emerged as an attempt to unify the attempts made to close upon the Hadamard conjecture which has generated a tremendous amount of research in combinatorial matrix theory in the last century. The theory of Hadamard matrices has a lot of applications. For example, in coding theory [22], difference sets [15], spectrometry [14], image processing, image coding, pattern recognition, sequence filtering [12], genetic algorithms [16], weighing designs for chemistry and medicine [5].

---

\*Supported in part by an internal research grant from Bar-Ilan University.

One of the tools for investigating Hadamard matrices is circulant weighing matrices. Circulant weighing matrices have been known to exist since 1975, when A.V. Geramita, J.M. Geramita and J. Seberry [9] observed the existence of a  $CW(7, 4)$  with first row

$$- \ + \ + \ 0 \ + \ 0 \ 0.$$

There are two major classification results of  $CW(n, k)$  for fixed weight  $k$ : One by R. Hain classifying  $CW(n, 4)$  [11], [8], and the other by Y. Strassler classifying  $CW(n, 9)$  [24], [27].

Here is a short list of previously known results about  $CW(n, 16)$ :

In 1975, Seberry and Whiteman [20] proved that  $CW(q^2 + q + 1, q^2) \neq \emptyset$  for  $q = p^\alpha$ ,  $p$  a prime,  $\alpha \geq 1$ . In particular, they constructed one  $CW(21, 16)$ .

In 1980, Eades [7] found a  $CW(31, 16)$  with first row

$$- \ 0 \ 0 \ 0 \ 0 \ - \ 0 \ + \ 0 \ - \ - \ + \ 0 \ + \ + \ 0 \ 0 \ 0 \ - \ + \ - \ + \ + \ 0 \ 0 \ + \ + \ 0 \ + \ 0 \ 0.$$

In 1995 (published 1998), Strassler [26] found another  $CW(31, 16)$ , not equivalent to the obtained by Eades.

In this paper we completely classify  $CW(n, 16)$ , for odd values of  $n$ . In the course of study, a new equivalence class was found in  $CW(63, 16)$ .

The paper has the following structure:

Definitions and known results appear in the Preliminaries Section (Section 2).

Section 3 contains the statement of a multiplier existence theorem, including a proof (essentially due to Muzychuk). This result is a starting point for the current work.

The other sections contain various steps of the actual classification process, attempting to find the possible describing sets  $P$  and  $N$  and the order  $n$  of a circulant weighing matrix of weight 16.

Section 4 introduces orbit length partitions, and contains a preliminary computation of all possible pairs of orbit length partitions of  $P$  and  $N$ .

Section 5 shortens the list of possible pairs by using restrictions on the number of short orbits.

Section 6 contains statements and proofs of general lemmas regarding orbit lengths of differences, which are then used to further reduce the number of possible pairs.

Section 7 contains a more delicate analysis of the remaining cases, using counting rather than existence arguments.

Section 8 contains final analysis of the few remaining cases, settling conclusively the questions of existence and equivalence. Computer search is used here.

The last section (Section 9) contains a summary of the results obtained.

## 2 Preliminaries

1. A *Hadamard matrix*  $H = (h_{ij})$  is a square matrix of order  $n$ , with entries  $h_{ij} \in \{-1, 1\}$ , satisfying  $HH^t = nI$ . Occasionally we refer to it as an  $H$  matrix.
2. The *Hadamard matrix conjecture*: Hadamard matrices exist for every order  $n$  divisible by 4 [20].

The conjecture's status: Still open, although many constructions of Hadamard matrices are known.

3. A generalization and construction aid: A *Weighing matrix*  $W = (w_{ij})$  of order  $n$  and weight  $k$  is a square matrix of order  $n$ , with entries  $w_{ij} \in \{0, 1, -1\}$ , satisfying

$$WW^t = kI_n.$$

$W(n, k)$  denotes the set of weighing matrices of order  $n$  and weight  $k$ . We use occasionally “ $W$  is a  $W(n, k)$ ” instead of “ $W \in W(n, k)$ ”. Also, occasionally we refer to it as a  $W$  matrix.

4. The *weighing matrix conjecture*: Weighing matrices exist for every order  $n$  divisible by 4 and all weights  $0 \leq k \leq n$  [22]. The conjecture's status: Still open, although many constructions of weighing matrices are known.
5. A basic construction for a weighing matrix  $W(n_1n_2, k_1k_2)$  is the *Kronecker product* of two weighing matrices  $W_1(n_1, k_1)$ ,  $W_2(n_2, k_2)$ . This is the block matrix

$$W = (w_{ij}) = ((W_1)_{ij}W_2)_{i,j=1}^{n_1}.$$

We denote this construction by  $W = W_1 \otimes W_2$ .

6. A *circulant matrix* is a square matrix in which each row (except the first) is a right cyclic shift of its predecessor. Since the first row of a circulant determines the whole

matrix we use the notation  $C = \text{cir}(c_0, c_1, \dots, c_{n-1})$  to denote the circulant matrix

$$\begin{pmatrix} c_0 & c_1 & \dots & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_{n-2} \\ \vdots & & & \\ c_1 & c_2 & \dots & c_0 \end{pmatrix}.$$

There are many different constructions for  $H$  and  $W$  matrices. Many of them use circulant matrices as construction aids.

7. A *circulant weighing matrix* is a circulant matrix which is also a weighing matrix.
8. Circulant weighing matrices as polynomials: Circulant matrices with integer entries form a ring under matrix addition and multiplication. This ring is isomorphic to the quotient ring  $R_n := \mathbf{Z}[x] / \langle x^n - 1 \rangle$ ; the natural isomorphism takes the matrix

$$\text{cir}(w_0, w_1, \dots, w_{n-1})$$

into the corresponding *Hall polynomial*

$$w_0 + w_1x + \dots + w_{n-1}x^{n-1}.$$

In the ring  $R_n$  the weighing property takes the form:

$$w(x)w(x^{-1}) = k,$$

where  $x^{-1} := x^{n-1}$ .

9.  $CW(n, k)$  denotes the set of circulant weighing matrices of order  $n$  and weight  $k$ . We use occasionally “ $W$  is a  $CW(n, k)$ ” instead of “ $W \in CW(n, k)$ ”.

Sometimes we identify the matrices in  $CW(n, k)$  with the corresponding Hall polynomials. We write “ $w(x) \in CW(n, k)$ ”, where  $w(x)$  is the Hall polynomial of a circulant weighing matrix of order  $n$  and weight  $k$ .

10.  $\mathbf{Z}_n$  denotes the ring of integers modulo  $n$ .
11.  $\mathbf{Z}_n^*$  denotes the multiplicative group of integers modulo  $n$ , i.e.

$$\mathbf{Z}_n^* = \{t \in \mathbf{Z}_n \mid \gcd(t, n) = 1\}.$$

12. The circulant weighing matrices  $w_1(x)$ ,  $w_2(x)$  are *equivalent* if they satisfy

$$w_2(x) = x^s w_1(x^t) \quad (\text{in } R_n)$$

for some  $s \in \mathbf{Z}_n$ ,  $t \in \mathbf{Z}_n^*$ .

13. If  $W \in CW(n, k)$  then also  $-W \in CW(n, k)$ . Convention: We refer only to one of  $W$ ,  $-W$ , the one that has more +1's than -1's.

14. If  $CW(n, k) \neq \emptyset$  then  $k = s^2$  for some nonnegative integer  $s$  [23].

15. For  $W = \text{cir}(w_0, w_1, \dots, w_{n-1}) \in CW(n, s^2)$  let

$P := \{i \mid w_i = 1\}$ , the *positive describing set* of  $W$ ;

$N := \{i \mid w_i = -1\}$ , the *negative describing set* of  $W$ .

Then, using convention (13) above:

$$|P| = \frac{s(s+1)}{2}, \quad |N| = \frac{s(s-1)}{2} \quad [23].$$

16. The *support* of  $w(x) \in CW(n, k)$  is the set

$$S = S(w) := \{i \mid w_i \neq 0\}.$$

Hence  $S = P \cup N$ .

17. A *multiplier* for the circulant weighing matrix  $w(x) \in CW(n, k)$  is a number  $t \in \mathbf{Z}_n^*$  such that there exists a shift  $s \in \mathbf{Z}_n$  satisfying

$$w(x) = x^s w(x^t).$$

If  $s = 0$  then we say that  $t$  is a *fixing* multiplier for the circulant  $w(x)$ . We consider  $t = 1$  as a *trivial* multiplier. From now on, writing “ $t$  is a multiplier” always means “ $t$  is a nontrivial multiplier”.

18. Let  $w(x) \in CW(n, k)$  have a multiplier  $t$  with shift  $s$ . Then

$$tN + s = N \quad \text{and} \quad tP + s = P.$$

In particular, if  $t$  fixes  $w(x)$  then it also fixes its positive and negative describing sets:  $tN = N$  and  $tP = P$  [27].

19. If  $w(x) \in CW(n, k)$  with  $\gcd(n, k) = 1$  has a multiplier  $t$ , then it is equivalent to some  $w'(x) \in CW(n, k)$  for which  $t$  is a fixing multiplier [27].

20. Let  $t \in \mathbf{Z}_n^*$ . A subset  $Z \subset \mathbf{Z}_n$  is called a  $t$ -orbit if there exists an element  $z \in \mathbf{Z}_n$  such that

$$Z = \{t^i z \pmod{n} \mid i \in \mathbf{Z}\}.$$

Denote by  $ol(z)$  the *orbit length* of  $z \in \mathbf{Z}_n$ , i.e., the number of elements in the  $t$ -orbit containing  $z$ .

21. A *multiset* is a “set” in which repetitions of elements are allowed. We distinguish it from a regular set by using brackets  $[]$  instead of braces  $\{\}$ . For example,

$$X = [a, a, b, c, c, c] = [a^2, b, c^3].$$

22. Two multisets can be merged together to form a new multiset by the *adjunction* ( $\&$ ) operation, which is the union with repetitions counted. For example,

$$X = [a^2, b, c^3], Y = [a, b^5, d]$$

$$X \& Y = [a^3, b^6, c^3, d].$$

23. For a multiset  $X \subseteq \mathbf{Z}_n$ ,

$$\triangle X := [x_1 - x_2 \mid x_1, x_2 \in X, x_1 \neq x_2].$$

24. For multisets  $X, Y \subseteq \mathbf{Z}_n$ ,

$$\overline{\triangle} X, Y := [\pm(x - y) \mid x \in X, y \in Y].$$

25. The CW multiset equation: If  $P$  and  $N$  are the (positive and negative) describing sets of some  $W \in CW(n, k)$  then

$$\triangle P \& \triangle N = \overline{\triangle} P, N \quad [27].$$

Note that  $P$  and  $N$  are sets, but  $\triangle P$ ,  $\triangle N$  and  $\overline{\triangle} P, N$  are (in general) multisets.

26. If  $q = 2^t$  and  $i$  is even then  $CW(\frac{q^{i+1}-1}{q-1}, q^i) \neq \emptyset$  [2], [3].

### 3 A Multiplier Existence Theorem

A fundamental result, on which the current classification is based, is the following multiplier existence theorem. This is by now a folklore result, quoted (and sometimes reproved) in many sources - e.g., McFarland [18], Lander [17], Arasu [4], Jungnickel [15], Muzychuk [19]. In order to make the paper self-contained, we include here a relatively short and elegant proof, basically due to Muzychuk [19], and adapted to suit our context.

**Theorem 3.1** *Let  $w(x) \in CW(n, k)$ ,  $k = s^2$ . If  $s = p^m$  for a prime  $p$  such that  $\gcd(n, p) = 1$  (and  $m \geq 1$ ), then  $p$  is a multiplier for  $w(x)$ .*

**Proof**

Let  $b$  be the maximal nonnegative integer such that

$$w(x^{p^j})w(x^{-1}) \equiv 0 \pmod{p^b} \quad (\text{in } R_n),$$

for all nonnegative integers  $j$ . Of course, since

$$w(x)w(x^{-1}) = k = p^{2m} \quad (\text{in } R_n),$$

necessarily  $b \leq 2m$ . We shall show that  $b = 2m$ .

Indeed, let  $j_0$  be a nonnegative integer such that

$$w(x^{p^{j_0}})w(x^{-1}) = p^b v_0(x)$$

for some  $v_0(x) \in R_n$  such that  $v_0(x) \not\equiv 0 \pmod{p}$ . Then

$$p^{2b} v_0(x^{p^{j_0}})v_0(x) = w(x^{p^{2j_0}})w(x^{-p^{j_0}})w(x^{p^{j_0}})w(x^{-1}) = w(x^{p^{2j_0}})w(x^{-1})p^{2m} \equiv 0 \pmod{p^{b+2m}},$$

by the definition of  $b$ . If  $b < 2m$  then it follows that

$$v_0(x^{p^{j_0}})v_0(x) \equiv 0 \pmod{p^{2m-b}}$$

so that, in particular (since  $v_0(x^p) \equiv v_0(x)^p \pmod{p}$ ):

$$v_0(x)^{p^{j_0+1}} \equiv v_0(x^{p^{j_0}})v_0(x) \pmod{p} \equiv 0 \pmod{p}.$$

It follows that  $v_0(x)$  is a nilpotent element in the ring  $\mathbf{Z}_p[x]/\langle x^n - 1 \rangle$ , which is the group algebra over  $\mathbf{Z}_p$  of the cyclic group of order  $n$ , and is therefore semisimple (since  $p \nmid n$ ). Thus  $v_0(x) \equiv 0 \pmod{p}$ , a contradiction. We have shown that  $b = 2m$ , and in particular (for  $j = 1$ ):

$$w(x^p)w(x^{-1}) \equiv 0 \pmod{p^{2m}} \quad (\text{in } R_n).$$

Let  $v(x) \in R_n$  satisfy

$$w(x^p)w(x^{-1}) = p^{2m}v(x) \quad (\text{in } R_n).$$

Then

$$p^{4m}v(x)v(x^{-1}) = w(x^p)w(x^{-1})w(x^{-p})w(x) = w(x^p)w(x^{-p})w(x)w(x^{-1}) = p^{2m}p^{2m}$$

so that

$$v(x)v(x^{-1}) = 1 \quad (\text{in } R_n).$$

Computing the coefficient of  $x^0 = 1$  on both sides of the equation, we conclude that if

$$v(x) = \sum_{i=0}^{n-1} v_i x^i \quad (v_i \in \mathbf{Z})$$

then

$$\sum_{i=0}^{n-1} v_i^2 = 1 \quad (\text{in } \mathbf{Z}).$$

Thus exactly one of the  $v_i$  is nonzero (and equal to  $\pm 1$ ), so that

$$w(x^p)w(x^{-1}) = p^{2m}v(x) = \pm p^{2m}x^i \quad (\text{in } R_n)$$

for some  $0 \leq i \leq n-1$ . Thus

$$\pm p^{2m}x^i w(x) = w(x^p)w(x^{-1})w(x) = w(x^p)p^{2m} \quad (\text{in } R_n),$$

$$\pm x^i w(x) = w(x^p) \quad (\text{in } R_n).$$

Obviously, the “ $\pm$ ” is actually “ $+$ ” (e.g., since the sum of the coefficients of  $w(x)$  is nonzero by (15) from Section 2). Therefore  $p$  is a multiplier for  $w(x)$ .

◇

## 4 Orbit-Length Partitions

The present work concerns  $CW(n, 16)$  where  $n$  is odd. Here  $k = s^2 = 16$ ,  $s = 4$ , and  $\gcd(n, 2) = 1$ . Thus, according to the multiplier existence theorem (Theorem 3.1),  $t = 2$  is a multiplier for each  $w(x) \in CW(n, 16)$ . By (15) in Section 2,

$$|P| = \frac{s(s+1)}{2} = \frac{4(4+1)}{2} = 10, \quad |N| = \frac{s(s-1)}{2} = \frac{4(4-1)}{2} = 6.$$

By claim (19) in Section 2 we can assume, without loss of generality, that  $t = 2$  is a fixing multiplier for  $w(x)$ . The sets  $P, N \subseteq \mathbf{Z}_n$  are then closed under multiplication by the multiplier  $t \in \mathbf{Z}_n^*$  (by claim (18)). It follows that  $P$  and  $N$  are unions of  $t$ -orbits.

Write now the  $t$ -orbits within  $P$  in order of increasing length, that is:  $P = C_1 \cup \cdots \cup C_m$ , where  $m$  is the number of  $t$ -orbits in  $P$ , and  $|C_i| \leq |C_{i+1}|$  ( $\forall i$ ). Denote  $l_i = |C_i|$  and obtain the *orbit length partition* of  $P$ :

$$olp(P) = (l_1, \dots, l_m) \quad (l_1 \leq \cdots \leq l_m).$$



If  $l_i = l_{i+1} = \dots = l_{i+d_i-1}$ , write  $l_i^{d_i}$  instead of  $d_i$  times  $l_i$ . We shall sometimes use the shorter notation

$$olp(P) = l_1^{d_1} l_2^{d_2} \dots l_k^{d_k} \quad (k \leq m)$$

instead of

$$olp(P) = (l_1^{d_1}, l_2^{d_2}, \dots, l_k^{d_k}) \quad (k \leq m).$$

Define  $olp(N)$  in a similar way.

#### Example 4.1

$$w(x) = -x + x^2 - x^3 + x^5 + x^6 + x^7 + x^8 - x^9 + x^{11} \in CW(13, 9).$$

This weighing circulant has  $t = 3$  as a multiplier.

$$|N| = 3, \quad |P| = 6.$$

$$N = \{1, 3, 9\}, \quad olp(N) = 3^1;$$

$$P = \{2, 6, 5, 8, 11, 7\} = C_1 \cup C_2, \quad \text{where } C_1 = \{2, 6, 5\} \text{ and } C_2 = \{8, 11, 7\}. \text{ Hence } olp(P) = 3^2.$$

Let us start by listing all possible partitions of  $N$  with  $|N| = 6$  and of  $P$  with  $|P| = 10$ :

$$olp(N) \in \{1^6, 1^4 2^1, 1^2 2^2, 2^3, 1^3 3^1, 1^1 2^1 3^1, 3^2, 1^2 4^1, 2^1 4^1, 1^1 5^1, 6^1\}.$$

$$olp(P) \in \{1^{10}, 1^8 2^1, 1^6 2^2, 1^4 2^3, 1^2 2^4, 2^5, 1^7 3^1, 1^5 2^1 3^1, 1^3 2^2 3^1, 1^1 2^3 3^1, 1^4 3^2, 1^2 2^1 3^2, 2^2 3^2, 1^1 3^3, 1^6 4^1, 1^4 2^1 4^1, 1^2 2^2 4^1, 2^3 4^1, 1^3 3^1 4^1, 1^1 2^1 3^1 4^1, 3^2 4^1, 1^2 4^2, 2^1 4^2, 1^5 5^1, 1^3 2^1 5^1, 1^1 2^2 5^1, 1^2 3^1 5^1, 2^1 3^1 5^1, 1^1 4^1 5^1, 5^2, 1^4 6^1, 1^2 2^1 6^1, 2^2 6^1, 1^1 3^1 6^1, 4^1 6^1, 1^3 7^1, 1^1 2^1 7^1, 3^1 7^1, 1^2 8^1, 2^1 8^1, 1^1 9^1, 10^1\}.$$

## 5 The Number of Short Orbits

Each of the  $t$ -orbits ( $t = 2$ ) encountered in the current classification has length at most 10. Therefore, if we determine for each  $1 \leq i \leq 10$  the number of orbits of length  $i$  in  $\mathbf{Z}_n$ , we shall be able to exclude orbit length partitions requiring more than this number of orbits, and thus reduce the size of our search space. It turns out that  $1 \leq i \leq 3$  suffice for the basic elimination process, but the cases  $4 \leq i \leq 6$  will also be needed in Section 7.

In general, an element  $a \in \mathbf{Z}_n$  has orbit length dividing  $i$  iff

$$2^i a \equiv a \pmod{n};$$

$$(2^i - 1)a \equiv 0 \pmod{n};$$

$$a = \frac{nk}{2^i - 1} \quad (k \in \{0, \dots, 2^i - 2\}).$$

Of course, to conclude that the orbit length is exactly  $i$ , one has to exclude all the proper divisors of  $i$ . This is easy when  $i$  is 1 or a prime number, and is not too difficult for other small values of  $i$ . We are interested in the cases  $1 \leq i \leq 6$ .

1.  $i = 1$ :

Let  $a \in \mathbf{Z}_n$  have  $ol(a) = 1$ . Then:

$$2^1 a \equiv a \pmod{n};$$

$$a \equiv 0 \pmod{n}.$$

Thus there is exactly one element in  $\mathbf{Z}_n$ , namely 0, whose orbit length is equal to 1.

2.  $i = 2$ :

Let  $a \in \mathbf{Z}_n$  have  $ol(a) = 2$ . Then:

$$2^2 a \equiv a \pmod{n};$$

$$3a \equiv 0 \pmod{n};$$

$$a = \frac{nk}{3} \quad (k \in \{0, 1, 2\}).$$

The value  $k = 0$  is impossible, since then  $a = 0$  and  $ol(a) = 1$ . Thus there are at most two elements in  $\mathbf{Z}_n$  with orbit length equal to 2. They form a single orbit:

$$\left(\frac{n}{3}, \frac{2n}{3}\right).$$

This orbit exists iff  $n$  is divisible by 3.

3.  $i = 3$ :

Let  $a \in \mathbf{Z}_n$  have  $ol(a) = 3$ . Then:

$$2^3 a \equiv a \pmod{n};$$

$$7a \equiv 0 \pmod{n};$$

$$a = \frac{nk}{7} \quad (k \in \{0, \dots, 6\}).$$

Again  $k = 0$  is impossible. Thus there are at most six elements in  $\mathbf{Z}_n$  with orbit length equal to 3. It follows that there are at most two orbits of length 3:

$$\left(\frac{n}{7}, \frac{2n}{7}, \frac{4n}{7}\right);$$

$$\left(\frac{3n}{7}, \frac{6n}{7}, \frac{5n}{7}\right).$$

Each of these orbits exists iff  $n$  is divisible by 7.

4.  $i = 4$ :

The orbit length of  $a \in \mathbf{Z}_n$  divides 4 iff

$$a = \frac{nk}{15} \quad (k \in \{0, \dots, 14\}).$$

The cases  $k \in \{0, 5, 10\}$  lead to shorter orbits (length 1 or 2). The cases  $k \in \{3, 6, 9, 12\}$  are possible whenever  $5 \mid n$ . Thus there is at least one orbit of length 4 in  $\mathbf{Z}_n$  iff  $n$  is divisible by 5, and there are three different orbits of length 4 iff  $n$  is divisible by 15.

5.  $i = 5$ :

The orbit length of  $a \in \mathbf{Z}_n$  divides 5 iff

$$2^5 a \equiv a \pmod{n};$$

$$31a \equiv 0 \pmod{n};$$

$$a = \frac{nk}{31} \quad (k \in \{0, \dots, 30\}).$$

The value  $k = 0$  leads to  $a = 0$  with orbit length 1. Thus there are at most 30 elements in  $\mathbf{Z}_n$  with orbit length equal to 5. In other words, there are at most  $30 \div 5 = 6$  orbits of length 5. Each of them exists iff  $n$  is divisible by 31.

6.  $i = 6$ :

The orbit length of  $a \in \mathbf{Z}_n$  divides 6 iff

$$2^6 a \equiv a \pmod{n};$$

$$a = \frac{nk}{63} \quad (k \in \{0, \dots, 62\}).$$

We have to exclude orbit length 1, 2 and 3 (the proper divisors of 6). Note that  $63 = 3 \times 3 \times 7$ . Using the analysis of previous cases, we get:

- $ol(a) = 1$  iff  $k = 0$ .

- $ol(a) = 2$  iff  $21|k$  and  $k \neq 0$ , i.e.  $k \in \{21, 42\}$ .
- $ol(a) = 3$  iff  $9|k$  and  $k \neq 0$ , i.e.  $k \in \{9, 18, 27, 36, 45, 54\}$ .

We are left with at most  $63 - (1 + 2 + 6) = 54$  elements in  $\mathbf{Z}_n$  with orbit length equal to 6. It follows that there are at most  $54 \div 6 = 9$  orbits of length 6.

Some of these orbits exist even if  $63 \nmid n$ . Indeed, if  $n$  is divisible by 63 then there are 9 orbits; if  $n$  is divisible by 21 but not by 63 then there are two orbits ( $3|k$  but  $9 \nmid k$  and  $21 \nmid k$ , i.e.,  $k \in \{3, 6, 12, 15, 24, 30, 33, 39, 48, 51, 57, 60\}$ ); and if  $n$  is divisible by 9 but not by 63 then there is only one orbit ( $7|k$  but  $21 \nmid k$ , i.e.,  $k \in \{7, 14, 28, 35, 49, 56\}$ ).

Let us return now to  $olp(P)$  and  $olp(N)$ . From the above analysis of the cases  $i \in \{1, 2, 3\}$  it follows that we can delete from our list all orbit length partitions that contain

$$1^a \text{ with } a > 1, \quad 2^a \text{ with } a > 1, \text{ or } 3^a \text{ with } a > 2.$$

Thus there remain only the following orbit length partitions :

$$olp(N) \in \{1^1 2^1 3^1, 3^2, 2^1 4^1, 1^1 5^1, 6^1\}.$$

$$olp(P) \in \{1^1 2^1 3^1 4^1, 3^2 4^1, 2^1 4^2, 2^1 3^1 5^1, 1^1 4^1 5^1, 5^2, 1^1 3^1 6^1, 4^1 6^1, 1^1 2^1 7^1, 3^1 7^1, 2^1 8^1, 1^1 9^1, 10^1\}.$$

Overall, we still have  $5 \times 13 = 65$  cases to check. Actually, the restrictions on the number of orbits of given size apply not only to each of  $olp(P)$  and  $olp(N)$  separately, but to the combined partition  $olp(P) \cup olp(N)$  as well.

Applying this condition, there remain only 41 possible pairs  $(olp(P), olp(N))$ :

**Table 1:** Initial list of pairs of orbit length partitions

#	$olp(P)$	$olp(N)$
1	$5^2$	$1^1 2^1 3^1$
2	$4^1 6^1$	$1^1 2^1 3^1$
3	$3^1 7^1$	$1^1 2^1 3^1$
4	$10^1$	$1^1 2^1 3^1$
5	$2^1 4^2$	$3^2$
6	$1^1 4^1 5^1$	$3^2$

#	$olp(P)$	$olp(N)$
7	$5^2$	$3^2$
8	$4^1 6^1$	$3^2$
9	$1^1 2^1 7^1$	$3^2$
10	$2^1 8^1$	$3^2$
11	$1^1 9^1$	$3^2$
12	$10^1$	$3^2$
13	$3^2 4^1$	$2^1 4^1$
14	$1^1 4^1 5^1$	$2^1 4^1$
15	$5^2$	$2^1 4^1$
16	$1^1 3^1 6^1$	$2^1 4^1$
17	$4^1 6^1$	$2^1 4^1$
18	$3^1 7^1$	$2^1 4^1$
19	$1^1 9^1$	$2^1 4^1$
20	$10^1$	$2^1 4^1$
21	$3^2 4^1$	$1^1 5^1$
22	$2^1 4^2$	$1^1 5^1$
23	$2^1 3^1 5^1$	$1^1 5^1$
24	$5^2$	$1^1 5^1$
25	$4^1 6^1$	$1^1 5^1$
26	$3^1 7^1$	$1^1 5^1$
27	$2^1 8^1$	$1^1 5^1$
28	$10^1$	$1^1 5^1$
29	$1^1 2^1 3^1 4^1$	$6^1$
30	$3^2 4^1$	$6^1$
31	$2^1 4^2$	$6^1$
32	$2^1 3^1 5^1$	$6^1$
33	$1^1 4^1 5^1$	$6^1$
34	$5^2$	$6^1$
35	$1^1 3^1 6^1$	$6^1$
36	$4^1 6^1$	$6^1$
37	$1^1 2^1 7^1$	$6^1$
38	$3^1 7^1$	$6^1$

#	$olp(P)$	$olp(N)$
39	$2^1 8^1$	$6^1$
40	$1^1 9^1$	$6^1$
41	$10^1$	$6^1$

## 6 Auxiliary Lemmas on Differences

In this section we shall formulate and prove lemmas, concerning orbit lengths of differences, that will be useful in eliminating more cases. Recall the notation  $ol(a)$  for the orbit length of  $a \in \mathbf{Z}_n$ .

**Observation 6.1** *If  $ol(a) = 1$  and  $ol(b) = k > 1$ , then  $ol(a - b) = k$ .*

Indeed, by the previous section  $a = 0$ , hence  $ol(a - b) = ol(-b) = ol(b) = k$ .

**Observation 6.2** *If  $a \neq b$ , then  $ol(a - b) > 1$ .*

Denote by  $gcd(a, b)$  the *greatest common divisor* and by  $lcm(a, b)$  the *least common multiple* of the integers  $a$  and  $b$ .

**Lemma 6.3** *If  $ol(a) = k$ ,  $ol(b) = l$  and  $ol(a - b) = m$  then*

1.  $m \mid lcm(k, l)$ ;
2.  $k \mid lcm(l, m)$ ;
3.  $l \mid lcm(m, k)$ ;

**Proof:**

1. Since  $t^k a = a$  and  $t^l b = b$ , it follows that  $t^{lcm(k, l)} a = a$  and  $t^{lcm(k, l)} b = b$  so that  $t^{lcm(k, l)}(a - b) = a - b$  as well. Since, for  $i \geq 0$ ,  $t^i(a - b) = a - b$  iff  $ol(a - b) \mid i$ , it follows that  $m = ol(a - b)$  divides  $lcm(k, l)$ .

2. Since  $a = b - (b - a)$  and  $ol(b - a) = ol(a - b) = m$ , replacing  $a, b, a - b$  by  $b, b - a, a$ , respectively, gives  $k \mid lcm(l, m)$ .
3. Similarly, since  $b = a - (a - b)$ , replacing  $a, b, a - b$  from the first case by  $a, a - b, b$ , respectively, gives  $l \mid lcm(m, k)$ .

◇

**Corollary 6.4** *If  $ol(a) = ol(b) = k$ ,  $a \neq b$ , and  $k$  is prime, then  $ol(a - b) = k$ .*

Indeed, by Lemma 6.3,  $ol(a - b) \mid k$ . Since  $k$  is prime,  $ol(a - b) = 1$  or  $ol(a - b) = k$ . The first option is impossible because  $a \neq b$ ; hence  $ol(a - b) = k$ .

**Lemma 6.5** *If  $ol(a) = k$ ,  $ol(b) = l$  and  $gcd(k, l) = 1$ , then  $ol(a - b) = kl$ .*

**Proof:**

Let  $m := ol(a - b)$ .

- By Lemma 6.3,  $m \mid lcm(k, l)$ ; but  $gcd(k, l) = 1$ , so that  $lcm(k, l) = kl$ . Hence  $m = k'l'$ , where  $k' \mid k$  and  $l' \mid l$ . We shall prove that  $k' = k$  and  $l' = l$ .
- $l \mid lcm(k, m)$ , by Lemma 6.3. Notice that  $gcd(k, l) = 1$ , hence  $l \mid m$ . Thus  $l' = l$ .
- $k \mid lcm(m, l)$ , by Lemma 6.3. In other words,  $k \mid lcm(k'l, l) = k'l$ . Notice that  $gcd(k, l) = 1$ , hence  $k \mid k'$ . Therefore  $k' = k$  and  $m = kl$ .

◇

**Lemma 6.6** *Let  $ol(a) = k$ ,  $ol(b) = m$ , and  $ol(a - b) = l$ . If  $m$  is prime then exactly one of the following holds:*

1.  $l = km$ ,  $m \nmid k$ .
2.  $l = k$ ,  $m \mid k$ .
3.  $l = \frac{k}{m}$ ,  $m \mid k$ ,  $m \nmid l$ .

**Proof:** It is clear that the three cases are mutually exclusive. Thus it suffices to show that at least one of them holds.

If  $m \nmid k$  then  $\gcd(k, m) = 1$ , hence by Lemma 6.5  $l = km$ . This gives case 1.

If  $m \mid k$  then one of the following holds: Either  $m \mid l$ , and then  $\text{lcm}(k, m) = k$  and  $\text{lcm}(l, m) = l$ . Thus, by Lemma 6.3,  $l \mid k$  and  $k \mid l$  and therefore  $l = k$ . This is case 2.

Alternatively,  $m \nmid l$ . Then  $\text{lcm}(k, m) = k$  and  $\text{lcm}(l, m) = lm$ , so that, by Lemma 6.3,  $l \mid k$  and  $k \mid lm$ . Writing  $k = k'm$ , we get  $l \mid k'm$  and  $k'm \mid lm$ . Hence  $l \mid k'$  and  $k' \mid l$ . Thus  $l = k' = \frac{k}{m}$ ,  $m \mid k$  but  $m \nmid l$ . This is case 3.

◇

**Lemma 6.7** *Let  $\text{ol}(a) = k$ ,  $\text{ol}(b) = m$ , and  $\text{ol}(a - b) = l$ . If  $k = k'u$  and  $m = m'u$  with  $\gcd(k', m') = 1$  and  $u$  prime then:*

1. *Either  $l = k'm'$  or  $l = uk'm'$ .*
2. *If either  $u \mid k'$  or  $u \mid m'$ , then  $l = uk'm'$ .*

**Proof:**

By Lemma 6.3,

$$k \mid \text{lcm}(l, m) \Rightarrow k'u \mid \text{lcm}(l, m'u) \xrightarrow{\gcd(k', m')=1} k' \mid l$$

and

$$m \mid \text{lcm}(l, k) \Rightarrow m'u \mid \text{lcm}(l, k'u) \xrightarrow{\gcd(k', m')=1} m' \mid l.$$

Hence  $k'm' \mid l$ .

1. Since  $\text{lcm}(k, m) = uk'm'$ , it follows from Lemma 6.3 that  $l \mid uk'm'$ . Since also  $k'm' \mid l$  and  $u$  is prime, it follows that either  $l = k'm'$  or  $l = uk'm'$ .
2. Assume, for example, that  $u \mid k'$ .

Write  $k' = uk''$ . By Lemma 6.3,  $k \mid \text{lcm}(l, m)$ . If  $l \neq uk'm'$  then

$$l = k'm' = uk''m' = k''m$$

and we obtain that  $\text{lcm}(l, m) = k''m$ . Hence  $k \mid k''m \Rightarrow k''u^2 \mid k''m \Rightarrow u^2 \mid m'u \Rightarrow u \mid m' \Rightarrow u \mid \gcd(k', m') \Rightarrow u = 1$ , contradicting the assumption that  $u$  is prime. Thus  $l = uk'm'$ .



◇

**Lemma 6.8** *Suppose that there are  $a \in P$  and  $b \in N$  so that  $ol(a) = k$  is prime,  $ol(b) = m \neq 1$ , and the following conditions hold:*

1.  $gcd(k, m) = 1$ ;
2.  $k \nmid y, \forall y \in olp(N)$ ;
3. *If  $m = m'm''$  with  $gcd(m', m'') = 1$  then, for each  $k', k'' \in olp(P)$ , either*

$$m' \nmid k' \quad \text{or} \quad m'' \nmid k''.$$

*Then these  $P$  and  $N$  do not define any circulant weighing matrix.*

**Proof:** Suppose that all the conditions are satisfied. Consider the element  $a - b \in \overline{\Delta}P, N$ .

From condition (1) it follow, by Lemma 6.5, that  $ol(a - b) = km$ . We shall show that there is no element in  $\Delta P \& \Delta N$  with orbit length equal to  $km$ , thus contradicting the multiset equation

$$\Delta P \& \Delta N = \overline{\Delta}P, N$$

of claim (25) in Section 2.

- Suppose that  $\bar{p} \in \Delta P$  has  $ol(\bar{p}) = km$ . Then  $\bar{p} = p_1 - p_2$ , where

$$p_1, p_2 \in P, p_1 \neq p_2, ol(p_i) = k_i, i = 1, 2.$$

By Lemma 6.3,  $km \mid lcm(k_1, k_2)$ . Since  $m \mid lcm(k_1, k_2)$ , there exist  $1 \leq m_1, m_2 \leq m$  such that  $m = m_1 m_2$ ,  $gcd(m_1, m_2) = 1$ ,  $m_1 \mid k_1$ ,  $m_2 \mid k_2$ . This contradicts condition (3).

- Suppose that  $\bar{q} \in \Delta N$  has  $ol(\bar{q}) = km$ . Then  $\bar{q} = q_1 - q_2$ , where

$$q_1, q_2 \in N, q_1 \neq q_2, ol(q_i) = m_i, i = 1, 2.$$

By Lemma 6.3,  $km \mid lcm(m_1, m_2)$ . Since  $k$  is prime, This implies that either  $k \mid m_1$  or  $k \mid m_2$ . Contradiction with condition (2).

◇

The above lemmas will now be used to analyze the multiset equation ((25) in Section 2)

$$\triangle P \& \triangle N = \overline{\triangle} P, N.$$

A necessary condition for equality to hold is:

*For each  $i$ , the number of elements in  $\triangle P \& \triangle N$  with orbit length equal to  $i$  is equal to the number of elements in  $\overline{\triangle} P, N$  with orbit length equal to  $i$ .*

For each multiset  $olp(P)$ , let  $pol(\triangle P)$  be the set of all *possible orbit lengths* in  $\triangle P$  obtained by using the above lemmas. Define similarly  $pol(\triangle N)$  from  $olp(N)$ . The following table lists the cases in which the multiset equation is false because

$$(\exists y_0 \in \overline{\triangle} P, N) (\forall x \in \triangle P \& \triangle N) ol(x) \neq ol(y_0).$$

**Table 2:** Pairs of orbit-length partitions rejected by use of lemmas

#	$olp(P)$	$pol(\triangle P)$	$olp(N)$	$pol(\triangle N)$	Rejected due to
1	$5^2$	$\{5\}$	$1^1 2^1 3^1$	$\{2, 3, 6\}$	Lemma 6.5: $k = 5, m = 2 \Rightarrow ol(y_0) = 10$
2	$4^1 6^1$	$\{2, 3, 4, 6, 12\}$	$1^1 2^1 3^1$	$\{2, 3, 6\}$	o. k.
3	$3^1 7^1$	$\{3, 7, 21\}$	$1^1 2^1 3^1$	$\{2, 3, 6\}$	Lemma 6.5: $k = 7, m = 2 \Rightarrow ol(y_0) = 14$
4	$10^1$	$\{2, 5, 10\}$	$1^1 2^1 3^1$	$\{2, 3, 6\}$	Lemma 6.5: $k = 10, m = 3 \Rightarrow ol(y_0) = 30$
5	$2^1 4^2$	$\{2, 4\}$	$3^2$	$\{3\}$	Lemma 6.5: $k = 2, m = 3 \Rightarrow ol(y_0) = 6$
6	$1^1 4^1 5^1$	$\{2, 4, 5, 20\}$	$3^2$	$\{3\}$	Lemma 6.5: $k = 4, m = 3 \Rightarrow ol(y_0) = 12$
7	$5^2$	$\{5\}$	$3^2$	$\{3\}$	Lemma 6.5: $k = 5, m = 3 \Rightarrow ol(y_0) = 15$
8	$4^1 6^1$	$\{2, 3, 4, 6, 12\}$	$3^2$	$\{3\}$	o. k.
9	$1^1 2^1 7^1$	$\{2, 7, 14\}$	$3^2$	$\{3\}$	Lemma 6.5: $k = 2, m = 3 \Rightarrow ol(y_0) = 6$
10	$2^1 8^1$	$\{2, 4, 8\}$	$3^2$	$\{3\}$	Lemma 6.5: $k = 2, m = 3 \Rightarrow ol(y_0) = 6$
11	$1^1 9^1$	$\{3, 9\}$	$3^2$	$\{3\}$	o. k.
12	$10^1$	$\{2, 5, 10\}$	$3^2$	$\{3\}$	Lemma 6.5: $k = 10, m = 3 \Rightarrow ol(y_0) = 30$
13	$3^2 4^1$	$\{2, 3, 4, 12\}$	$2^1 4^1$	$\{2, 4\}$	Lemma 6.5: $k = 3, m = 2 \Rightarrow ol(y_0) = 6$
14	$1^1 4^1 5^1$	$\{2, 4, 5, 20\}$	$2^1 4^1$	$\{2, 4\}$	Lemma 6.5: $k = 5, m = 2 \Rightarrow ol(y_0) = 10$
15	$5^2$	$\{5\}$	$2^1 4^1$	$\{2, 4\}$	Lemma 6.5: $k = 5, m = 2 \Rightarrow ol(y_0) = 10$
16	$1^1 3^1 6^1$	$\{2, 3, 6\}$	$2^1 4^1$	$\{2, 4\}$	Lemma 6.5: $k = 3, m = 4 \Rightarrow ol(y_0) = 12$
17	$4^1 6^1$	$\{2, 3, 4, 6, 12\}$	$2^1 4^1$	$\{2, 4\}$	o. k.
18	$3^1 7^1$	$\{3, 7, 21\}$	$2^1 4^1$	$\{2, 4\}$	Lemma 6.5: $k = 3, m = 2 \Rightarrow ol(y_0) = 6$
19	$1^1 9^1$	$\{3, 9\}$	$2^1 4^1$	$\{2, 4\}$	Lemma 6.5: $k = 9, m = 2 \Rightarrow ol(y_0) = 18$
20	$10^1$	$\{2, 5, 10\}$	$2^1 4^1$	$\{2, 4\}$	Lemma 6.7: $k = 10, m = 4, u = 2 \Rightarrow ol(y_0) = 20$
21	$3^2 4^1$	$\{2, 3, 4, 12\}$	$1^1 5^1$	$\{5\}$	Lemma 6.5: $k = 3, m = 5 \Rightarrow ol(y_0) = 15$

#	$olp(P)$	$pol(\triangle P)$	$olp(N)$	$pol(\triangle N)$	Rejected due to
22	$2^1 4^2$	$\{2,4\}$	$1^1 5^1$	$\{5\}$	Lemma 6.5: $k = 2, m = 5 \Rightarrow ol(y_0) = 10$
23	$2^1 3^1 5^1$	$\{2,3,5,6,10,15\}$	$1^1 5^1$	$\{5\}$	o. k.
24	$5^2$	$\{5\}$	$1^1 5^1$	$\{5\}$	o. k.
25	$4^1 6^1$	$\{2,3,4,6,12\}$	$1^1 5^1$	$\{5\}$	Lemma 6.5: $k = 4, m = 5 \Rightarrow ol(y_0) = 20$
26	$3^1 7^1$	$\{3,7,21\}$	$1^1 5^1$	$\{5\}$	Lemma 6.5: $k = 3, m = 5 \Rightarrow ol(y_0) = 15$
27	$2^1 8^1$	$\{2,4,8\}$	$1^1 5^1$	$\{5\}$	Lemma 6.5: $k = 2, m = 5 \Rightarrow ol(y_0) = 10$
28	$10^1$	$\{2,5,10\}$	$1^1 5^1$	$\{5\}$	o. k.
29	$1^1 2^1 3^1 4^1$	$\{2,3,4,6,12\}$	$6^1$	$\{2,3,6\}$	o. k.
30	$3^2 4^1$	$\{2,3,4,12\}$	$6^1$	$\{2,3,6\}$	o. k.
31	$2^1 4^2$	$\{2,4\}$	$6^1$	$\{2,3,6\}$	Lemma 6.7: $k = 4, m = 6, u = 2 \Rightarrow ol(y_0) = 12$
32	$2^1 3^1 5^1$	$\{2,3,5,6,10,15\}$	$6^1$	$\{2,3,6\}$	Lemma 6.5: $k = 5, m = 6 \Rightarrow ol(y_0) = 30$
33	$1^1 4^1 5^1$	$\{2,4,5,20\}$	$6^1$	$\{2,3,6\}$	Lemma 6.5: $k = 5, m = 6 \Rightarrow ol(y_0) = 30$
34	$5^2$	$\{5\}$	$6^1$	$\{2,3,6\}$	Lemma 6.5: $k = 5, m = 6 \Rightarrow ol(y_0) = 30$
35	$1^1 3^1 6^1$	$\{2,3,6\}$	$6^1$	$\{2,3,6\}$	o. k.
36	$4^1 6^1$	$\{2,3,4,6,12\}$	$6^1$	$\{2,3,6\}$	o. k.
37	$1^1 2^1 7^1$	$\{2,7,14\}$	$6^1$	$\{2,3,6\}$	Lemma 6.5: $k = 7, m = 6 \Rightarrow ol(y_0) = 42$
38	$3^1 7^1$	$\{3,7,21\}$	$6^1$	$\{2,3,6\}$	Lemma 6.5: $k = 7, m = 6 \Rightarrow ol(y_0) = 42$
39	$2^1 8^1$	$\{2,4,8\}$	$6^1$	$\{2,3,6\}$	Lemma 6.7: $k = 8, m = 6, u = 2 \Rightarrow ol(y_0) = 24$
40	$1^1 9^1$	$\{3,9\}$	$6^1$	$\{2,3,6\}$	Lemma 6.7: $k = 9, m = 6, u = 3 \Rightarrow ol(y_0) = 18$
41	$10^1$	$\{2,5,10\}$	$6^1$	$\{2,3,6\}$	Lemma 6.7: $k = 10, m = 6, u = 2 \Rightarrow ol(y_0) \in \{15, 30\}$

## 7 Counting Arguments

There now remain only a small number of cases.

**Table 3:** Pairs of orbit-length partitions surviving the lemmas

#	$olp(P)$	$olp(N)$
1	$4^1 6^1$	$1^1 2^1 3^1$
2	$4^1 6^1$	$3^2$
3	$1^1 9^1$	$3^2$
4	$4^1 6^1$	$2^1 4^1$

#	$olp(P)$	$olp(N)$
5	$2^1 3^1 5^1$	$1^1 5^1$
6	$5^2$	$1^1 5^1$
7	$10^1$	$1^1 5^1$
8	$1^1 2^1 3^1 4^1$	$6^1$
9	$3^2 4^1$	$6^1$
10	$1^1 3^1 6^1$	$6^1$
11	$4^1 6^1$	$6^1$

In this section we shall subject these cases to a more delicate analysis. In most cases, counting arguments will be used instead of simple existence considerations.

Let  $\langle a \rangle$  denote the  $z$ -orbit of  $a \in \mathbf{Z}_n$ . Denote also

$$\mathbf{OL}(\langle \mathbf{a} \rangle - \langle \mathbf{a} \rangle) := \{ol(2^i a - 2^j a) \mid i \neq j, 0 \leq i, j \leq ol(a) - 1\};$$

and for  $\langle a \rangle \neq \langle b \rangle$

$$\mathbf{OL}(\langle \mathbf{a} \rangle - \langle \mathbf{b} \rangle) := \{ol(2^i a - 2^j b) \mid 0 \leq i \leq ol(a) - 1, 0 \leq j \leq ol(b) - 1\}.$$

Note that  $OL(\langle a \rangle - \langle a \rangle)$  and  $OL(\langle a \rangle - \langle b \rangle)$  are sets of positive integers. When we write below  $ol(\langle a \rangle - \langle a \rangle)$  or  $ol(\langle a \rangle - \langle b \rangle)$  we mean an arbitrary element of the corresponding set. We shall now analyze all the cases in the above table, one by one.

1.  $P = \{a, 2a, 4a, 8a, b, 2b, 4b, 8b, 16b, 32b\}$ ;  $N = \{c, d, 2d, e, 2e, 4e\}$ ;  
 $ol(a) = 4$ ,  $ol(b) = 6$ ;  $ol(c) = 1$ ,  $ol(d) = 2$ ,  $ol(e) = 3$ .

Let us count the elements with orbit length 12 in  $\triangle P \& \triangle N$  and in  $\overline{\triangle} P, N$ . By Lemma 6.7  $ol(\langle a \rangle - \langle b \rangle) = 12$  and by Lemma 6.5  $ol(\langle a \rangle - \langle e \rangle) = 12$ . It easy to see that no other combinations of the orbit lengths in this case yields 12. Therefore the number of elements with orbit length 12 in  $\triangle P \& \triangle N$  is  $2 \times 4 \times 6 = 48$  and in  $\overline{\triangle} P, N$  it is  $2 \times 4 \times 3 = 24$ . Thus, we obtain the contradiction

$$\overline{\triangle} P, N \neq \triangle P \& \triangle N.$$

2.  $P = \{a, 2a, 4a, 8a, b, 2b, 4b, 8b, 16b, 32b\}$ ;  $N = \{c, 2c, 4c, d, 2d, 4d\}$ ;  
 $ol(a) = 4$ ,  $ol(b) = 6$ ;  $ol(c) = 3$ ,  $ol(d) = 3$ .

$$\triangle P \& \triangle N :$$

$$\triangle P : ol(\langle b \rangle - \langle b \rangle) \in \{2, 3, 6\}, \text{ by Lemma 6.3 and Observation 6.2.}$$

$\triangle N : ol(\langle c \rangle - \langle c \rangle) = ol(\langle c \rangle - \langle d \rangle) = ol(\langle d \rangle - \langle d \rangle) = 3$ , by Corollary 6.4.

$\overline{\triangle}P, N$ :

$$ol(\langle a \rangle - \langle c \rangle) = ol(\langle a \rangle - \langle d \rangle) = 12, \text{ by Lemma 6.5.}$$

$$ol(\langle b \rangle - \langle c \rangle), ol(\langle b \rangle - \langle d \rangle) \in \{2, 6\}, \text{ by Lemma 6.6.}$$

Thus there is no element in  $\overline{\triangle}P, N$  whose orbit length is equal to 3. Hence, we conclude that  $\overline{\triangle}P, N \neq \triangle P \& \triangle N$ .

3.  $P = \{a, b, 2b, 4b, 8b, 16b, 32b, 64b, 128b, 256b\}$ ;  $N = \{c, 2c, 4c, d, 2d, 4d\}$ ;  
 $ol(a) = 1, ol(b) = 9; ol(c) = 3, ol(d) = 3$ .

$$\triangle N : ol(\langle c \rangle - \langle c \rangle) = ol(\langle c \rangle - \langle d \rangle) = ol(\langle d \rangle - \langle d \rangle) = 3, \text{ by Corollary 6.4}$$

and the number of these elements is  $3 \times 2 + 2 \times 3 \times 3 + 3 \times 2 = 30$ ;

$$\overline{\triangle}P, N : ol(\langle a \rangle - \langle c \rangle) = ol(\langle a \rangle - \langle d \rangle) = 3, \text{ by Observation 6.1}$$

and the number of these elements is  $2 \times 1 \times 3 + 2 \times 1 \times 3 = 12$ ;

$$ol(\langle b \rangle - \langle c \rangle) = ol(\langle b \rangle - \langle d \rangle) = 9, \text{ by Lemma 6.6.}$$

Thus the number of elements in  $\overline{\triangle}P, N$  whose orbit length is equal to 3 is smaller than the number of such elements in  $\triangle P \& \triangle N$ . Hence, we obtain that  $\overline{\triangle}P, N \neq \triangle P \& \triangle N$ .

4.  $P = \{a, 2a, 4a, 8a, b, 2b, 4b, 8b, 16b, 32b\}$ ;  $N = \{c, 2c, d, 2d, 4d, 8d\}$ ;  
 $ol(a) = 4, ol(b) = 6; ol(c) = 2, ol(d) = 4$ .

In this case we do not get a contradiction by using the lemmas from the Section 6, and this case remains as a candidate to be dealt with in the next section.

5.  $P = \{a, 2a, b, 4b, 8b, c, 2c, 4c, 8c, 16c\}$ ;  $N = \{d, e, 2e, 4e, 8e, 16e\}$ ;  
 $ol(a) = 2, ol(b) = 3, ol(c) = 5; ol(d) = 1, ol(e) = 5$ .

$$\triangle P : ol(\langle a \rangle - \langle b \rangle) = 6, \text{ by Lemma 6.5.}$$

It is easy to check that there is no element in  $\overline{\triangle}P, N$  whose orbit length is equal to 6. Hence, we conclude that  $\overline{\triangle}P, N \neq \triangle P \& \triangle N$ .

6.  $P = \{a, 2a, 4a, 8a, 16a, b, 2b, 4b, 8b, 16b\}$ ;  $N = \{c, d, 2d, 4d, 8d, 16d\}$ ;

$$ol(a) = 5, ol(b) = 5; ol(c) = 1, ol(d) = 5.$$

None of the lemmas leads to a contradiction in this case. Therefore this case still remains as a candidate.

7.  $P = \{a, 2a, 4a, 8a, 16a, 32a, 64a, 128a, 256a, 511a\}$ ;  $N = \{b, c, 2c, 4c, 8c, 16c\}$ ;

$$ol(a) = 10; ol(b) = 1, ol(c) = 5.$$

$$\triangle N : ol(\langle b \rangle - \langle c \rangle) = 5, \text{ by Observation 6.1.}$$

$\overline{\triangle}P, N$ :

$$ol(\langle a \rangle - \langle b \rangle) = 10, \text{ by Observation 6.1;}$$

$$ol(\langle a \rangle - \langle c \rangle) \in \{2, 10\}, \text{ by Lemma 6.6.}$$

Thus there is no element in  $\overline{\triangle}P, N$  with orbit length equal to 5. Hence, we conclude that  $\overline{\triangle}P, N \neq \triangle P \& \triangle N$ .

8.  $P = \{a, b, 2b, c, 2c, 4c, d, 2d, 4d, 8d\}$ ;  $N = \{e, 2e, 4e, 8e, 16e, 32e\}$ ;

$$ol(a) = 1, ol(b) = 2, ol(c) = 3, ol(d) = 4; ol(e) = 6.$$

$$\triangle P : ol(\langle c \rangle - \langle d \rangle) = 12, \text{ by Lemma 6.5,}$$

and these are the only elements in  $\triangle P$  with orbit length 12. Clearly, there are no elements of orbit length 12 in  $\triangle N$ .

$$\overline{\triangle}P, N : ol(\langle d \rangle - \langle e \rangle) = 12, \text{ by Lemma 6.7,}$$

and there are no other such elements in  $\overline{\triangle}P, N$ . Thus, we obtain that in  $\overline{\triangle}P, N$  there are  $2 \times (4 \times 6) = 48$  elements whose orbit length is equal to 12, while in  $\triangle P \& \triangle N$  there are only  $2 \times (3 \times 4) = 24$  such elements. Hence,  $\overline{\triangle}P, N \neq \triangle P \& \triangle N$ .

9.  $P = \{a, 2a, 4a, b, 2b, 4b, c, 2c, 4c, 8c\}$ ;  $N = \{d, 2d, 4d, 8d, 16d, 32d\}$ ;

$$ol(a) = 3, ol(b) = 3, ol(c) = 4; ol(d) = 6.$$

$$\triangle P : ol(\langle a \rangle - \langle a \rangle) = ol(\langle a \rangle - \langle b \rangle) = ol(\langle b \rangle - \langle b \rangle) = 3, \text{ by Corollary 6.4,}$$

but there is no element in  $\overline{\triangle}P, N$  whose orbit length is equal to 3 (may be shown using lemmas 6.6 and 6.7). Hence,  $\overline{\triangle}P, N \neq \triangle P \& \triangle N$ .

10.  $P = \{a, b, 2b, 4b, c, 2c, 4c, 8c, 16c, 32c\}$ ;  $N = \{d, 2d, 4d, 8d, 16d, 32d\}$ ;  
 $ol(a) = 1$ ,  $ol(b) = 3$ ,  $ol(c) = 6$ ;  $ol(d) = 6$ .

None of the lemmas leads to a contradiction in this case, and it remains as a candidate.

11.  $P = \{a, 2a, 4a, 8a, b, 2b, 4b, 8b, 16b, 32b\}$ ;  $N = \{c, 2c, 4c, 8c, 16c, 32c\}$ ;  
 $ol(a) = 4$ ,  $ol(b) = 6$ ;  $ol(c) = 6$ .

$$\triangle P : ol(\langle a \rangle - \langle a \rangle) \in \{2, 4\}, \text{ by Lemma 6.3 and Observation 6.2.}$$

Note that  $ol(2a - a) = ol(a) = 4$ , so there is at least one element of orbit length 4 in  $\triangle P$  and therefore in  $\triangle P \& \triangle N$ . On the other hand, there are no elements of orbit length 4 in  $\overline{\triangle P}, N$ . Hence,  $\overline{\triangle P}, N \neq \triangle P \& \triangle N$ .

## 8 Final Analysis

In this section we shall analyze more closely the three cases that survived the previous inspection (cases 4, 6 and 10). Let us list them again, in a different order:

1.  $olp(P) = 5^2$ ,  $olp(N) = 1^1 5^1$ .
2.  $olp(P) = 1^1 3^1 6^1$ ,  $olp(N) = 6^1$ .
3.  $olp(P) = 4^1 6^1$ ,  $olp(N) = 2^1 4^1$ .

Before embarking upon the detailed, examination of these cases, we need some general theorems.

**Theorem 8.1** *Suppose that  $A$  is a  $v \times v$  weighing matrix with  $v = km$  which has the block form:*

$$\begin{pmatrix} W & 0 & \dots & 0 \\ 0 & W & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & W \end{pmatrix}$$

*where  $W$  is a circulant  $m \times m$  matrix. Then there is a  $v \times v$  permutation matrix  $P$  such that  $P^{-1}AP$  is a circulant weighing matrix.*

**Proof:** Let  $A = (a_{ij})$  and  $W = (w_{ij})$  be the above matrices. Let  $P = (p_{ij})_{i,j=0}^{v-1}$  be the  $v \times v$  permutation matrix defined by:

$$p_{ij} = 1 \iff i = rm + s, j = sk + r \text{ for some } 0 \leq r \leq k-1, 0 \leq s \leq m-1.$$

Multiplying the matrix  $A$  by  $P^{-1}$  on the left turns row  $rm + s$  of the matrix  $A$  into row  $sk + r$ , while multiplying  $A$  by  $P$  on the right turns column  $rm + s$  of the matrix  $A$  into column  $sk + r$ . We'll prove now that  $B := P^{-1}AP$  is a circulant weighing matrix. Because permutation of rows and columns of a weighing matrix gives a weighing matrix, we only have to prove that  $B$  is circulant. In order to do so, we will prove that

$$b_{ij} = b_{i+1,j+1} \quad (\forall \quad 0 \leq i, j \leq v-1),$$

where addition of indices is modulo  $v$ . Let

$$i = s_1k + r_1 \quad \text{and} \quad j = s_2k + r_2 \quad (0 \leq r_1, r_2 \leq k-1, 0 \leq s_1, s_2 \leq m-1).$$

Then

$$i+1 = s_1k + r_1 + 1 \quad \text{and} \quad j+1 = s_2k + r_2 + 1.$$

The following table shows which rows and columns of the matrix  $A$  correspond to given rows and columns of the matrix  $B$ .

Matrix B	Matrix A
row $i$	row $r_1m + s_1$
column $j$	column $r_2m + s_2$
row $i+1$	row $(r_1+1)m + s_1$ , if $r_1 \neq k-1$
	row $0 \cdot m + (s_1+1)$ , if $r_1 = k-1$ , $s_1 \neq m-1$
	row $0 \cdot m + 0$ , if $r_1 = k-1$ , $s_1 = m-1$
column $j+1$	column $(r_2+1)m + s_2$ , if $r_2 \neq k-1$
	column $0 \cdot m + (s_2+1)$ , if $r_2 = k-1$ , $s_2 \neq m-1$
	column $0 \cdot m + 0$ , if $r_2 = k-1$ , $s_2 = m-1$

Thus the following cases are possible:

- $r_1 = r_2$ .

In this case row  $r_1m + s_1$  of  $A$  is row  $s_1$  in diagonal block number  $r_1$ , and column



$r_2m + s_2$  is column  $s_2$  in the same block. Hence

$$b_{ij} = a_{(r_1m+s_1), (r_2m+s_2)} = w_{s_1s_2}.$$

If  $r_1 \neq k-1$  then

$$b_{(i+1), (j+1)} = a_{((r_1+1)m+s_1), ((r_2+1)m+s_2)} = w_{s_1s_2}.$$

Otherwise,  $r_1 = k-1$  and

$$b_{(i+1), (j+1)} = a_{(0 \cdot m + (s_1+1)), (0 \cdot m + (s_2+1))} = w_{(s_1+1), (s_2+1)} = w_{s_1s_2}.$$

The last equality follows from  $W$  being circulant. Here  $s_1 + 1$  and  $s_2 + 1$  are taken modulo  $m$ , covering also the cases where

$$s_1 = m-1 \quad \text{or} \quad s_2 = m-1 \quad (\text{or both}).$$

Hence in all cases  $b_{ij} = b_{(i+1)(j+1)}$ .

•  $r_1 \neq r_2$ .

In this case the entry in row  $r_1m + s_1$  and column  $r_2m + s_2$  does not belong to a diagonal block of  $A$ .

Hence

$$b_{ij} = a_{(r_1m+s_1), (r_2m+s_2)} = 0.$$

If  $r_1 \neq k-1$  and  $r_2 \neq k-1$  then, similarly,

$$b_{(i+1), (j+1)} = a_{((r_1+1)m+s_1), ((r_2+1)m+s_2)} = 0.$$

Otherwise, with no loss of generality suppose that  $r_1 \neq k-1$  and  $r_2 = k-1$ . then

$$b_{(i+1), (j+1)} = a_{((r_1+1)m+s_1), (0 \cdot m + (s_2+1))} = 0.$$

Hence again  $b_{ij} = b_{(i+1), (j+1)}$ .

We have proved that

$$b_{ij} = b_{i+1, j+1} \quad (\forall \quad 0 \leq i, j \leq v-1)$$

and therefore the weighing matrix  $B$  is circulant.

◇

**Theorem 8.2** *If  $CW(n, k) \neq \emptyset$  then  $CW(mn, k) \neq \emptyset$  for every  $m \geq 1$ .*

**Proof:** Let  $W \in CW(n, k)$  and let  $I_m$  be the identity matrix of order  $m \geq 1$ . Note that  $I_m$  is a circulant weighing matrix of order  $m$  and weight 1. Hence the Kronecker product of these matrices gives the matrix  $W' = I_m \otimes W \in W(mn, k)$ :

$$W' = \begin{pmatrix} W & 0 & \dots & 0 \\ 0 & W & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & W \end{pmatrix}$$

By the previous Theorem 8.1 there is an  $mn \times mn$  permutation matrix  $P$  such that  $P^{-1}W'P \in CW(mn, k)$ . Thus  $CW(mn, k) \neq \emptyset$ .

◇

In the sequel we shall attempt to prove a converse to Theorem 7.2, but this will be done separately for each of the cases at hand. In each case we shall assume a specific pairs  $(olp(P), olp(N))$ .

We now proceed with the analysis of the above three cases.

1.  $P = \{a, 2a, 4a, 8a, 16a, b, 2b, 4b, 8b, 16b\}$ ;  $N = \{c, d, 2d, 4d, 8d, 16d\}$ ;  
 $ol(a) = 5$ ,  $ol(b) = 5$ ;  $ol(c) = 1$ ,  $ol(d) = 5$ .

$P$  and  $N$  contain orbits of lengths 1 and 5. In Section 5 we found necessary and sufficient conditions on  $n$  for the existence of an element in  $\mathbf{Z}_n$  with orbit length equal to  $i$ , for each  $1 \leq i \leq 6$ . In the present case,  $n$  must satisfy the conditions for  $i = 1$  and  $i = 5$ .

- $i = 1$ :  $n$  arbitrary.
- $i = 5$ :  $n$  must be divisible by 31.

We may thus assume that  $n = 31m$  for some (odd) integer  $m$ . We shall now state and prove a converse to Theorem 7.2, especially for the current case.

**Theorem 8.3**

(i) For each odd  $m \geq 1$ , if  $w(x) \in CW(31m, 16)$  has (for the multiplier  $t = 2$ )

$$olp(P) = 5^2, \quad olp(N) = 1^1 5^1$$

then there exists  $w_0(x) \in CW(31, 16)$  such that

$$w(x) = w_0(x^m).$$

(ii) If  $w_0(x^m)$ ,  $\tilde{w}_0(x^m)$  are equivalent in  $CW(31m, 16)$  then  $w_0(x)$ ,  $\tilde{w}_0(x)$  are equivalent in  $CW(31, 16)$

**Proof:**

(i) Let  $m \geq 1$  be an odd integer and assume that  $w(x) \in CW(31m, 16)$  with the given  $olp(P)$ ,  $olp(N)$ . Then the unique element with orbit length equal to 1 is  $0 \in N$ . Let  $x \in N$  and  $y, z \in P$  be generators for the three orbits of length 5. According to Section 5,

$$x = mk$$

for some  $1 \leq k \leq 30$ . Similarly,

$$y = mk', \quad z = mk''$$

for some  $1 \leq k', k'' \leq 30$ . Thus

$$m|s \quad (\forall s \in P \cup N)$$

so that there is a (unique) polynomial  $w_0(x) \in R_{31}$  such that

$$w(x) = w_0(x^m).$$

Clearly,  $w_0(x) \in CW(31, 16)$ .

(ii) Let  $w_0(x)$ ,  $\tilde{w}_0(x) \in CW(31, 16)$  be such that the polynomials  $w_0(x^m)$ ,  $\tilde{w}_0(x^m) \in CW(31m, 16)$  are equivalent. Thus there exist  $s \in \mathbf{Z}_{31m}$  and  $t \in \mathbf{Z}_{31m}^*$  such that

$$\tilde{w}_0(x^m) = x^s w_0(x^{mt}) \quad (\text{in } R_{31m}).$$

All the powers of  $x$  with non-zero coefficients in  $\tilde{w}_0(x^m)$  or  $w_0(x^{mt})$  are divisible by  $m$ . Therefore  $s = ms_1$  for a suitable  $s_1 \in \mathbf{Z}_{31}$ , and we conclude that

$$\tilde{w}_0(x) = x^{s_1} w_0(x^t) \quad (\text{in } R_{31}).$$

Note that  $t \in \mathbf{Z}_{31m}^*$  may also be viewed as  $t \in \mathbf{Z}_{31}^*$ .

◇

We now face the problem of finding all  $w(x) \in CW(31, 16)$  with the above  $olp(P)$  and  $olp(N)$ , and sorting them into equivalence classes. The data that we have are

$$n = 31, \quad k = 16, \quad t = 2, \quad olp(P) = 5^2, \quad olp(N) = 1^1 5^1.$$

We will find  $P$  and  $N$  with the help of a computer program. We are looking for  $w(x) = w_0 + w_1x + \cdots + w_{30}x^{30} \in CW(31, 16)$  with  $w_0 = -1$  ( $0 \in N$  since only 0 has orbit length equal to 1). The indices  $i$  for all the other nonzero  $w_i$  belong to orbits of length 5. According to Section 5, there are six different orbits of length 5 in  $\mathbf{Z}_{31}$ . For our  $w(x)$  we need three of them. Thus the Pascal program must check  $6 \binom{5}{2} = 60$  cases. Each case gives explicit  $P$  and  $N$  and therefore also  $w(x) \in R_{31}$  which defines a circulant  $\{0, 1, -1\}$ -matrix. In order to verify that this is a weighing matrix, we have to check the following conditions:

- $\sum_{i=0}^{30} w_i^2 = 16$ ;
- $\sum_{i=0}^{30} w_i w_{i+j} = 0, \quad 1 \leq j \leq 30$ ;

Note that the first condition is automatically satisfied (since  $w_i = \pm 1$ ); and in the second condition it is sufficient to check only cases up to  $j = \lfloor \frac{31}{2} \rfloor$ , since the other values of  $j$  are complements of these to 31. Hence for every candidate  $w(x)$  the program should make 15 comparisons.

This program was written and run, finding altogether 12 solutions. The list of solutions in  $CW(31, 16)$  includes all those previously obtained by R. Eades [7] and by Y. Strassler [26]. Another program designed to check possible equivalence between the matrices obtained. It showed that every  $w(x) \in CW(31, 16)$  is equivalent to one of the following two:

- (a)  $w_1(x) = -1 - x^1 - x^2 + x^3 - x^4 + x^6 + x^7 - x^8 + x^{12} + x^{14} - x^{16} + x^{17} + x^{19} + x^{24} + x^{25} + x^{28},$
- (b)  $w_2(x) = -1 - x^1 - x^2 - x^4 + x^5 - x^8 + x^9 + x^{10} + x^{15} - x^{16} + x^{18} + x^{20} + x^{23} + x^{27} + x^{29} + x^{30}.$

It is easy to see that  $w_1(x)$  and  $w_2(x)$  are inequivalent. Indeed, by Section 5 there are exactly 6 different orbits of length 5 in  $\mathbf{Z}_{31}$ . These are

$$C_0 = \{1, 2, 4, 8, 16\},$$

$$C_1 = \{3, 6, 12, 24, 17\},$$

$$C_2 = \{5, 10, 20, 9, 18\},$$

$$C_3 = \{7, 14, 28, 25, 19\},$$

$$C_4 = \{11, 22, 13, 26, 21\},$$

$$C_5 = \{15, 30, 29, 27, 23\}.$$

Denote by  $C_\infty = \{0\}$  the unique orbit of length 1.

Thus we obtain

- $w_1(x)$ :

$$P_1 = \{3, 6, 7, 12, 14, 17, 19, 24, 25, 28\} = C_1 \cup C_3,$$

$$N_1 = \{0, 1, 2, 4, 8, 16\} = C_\infty \cup C_0;$$

- $w_2(x)$ :

$$P_2 = \{5, 9, 10, 15, 18, 20, 23, 27, 29, 30\} = C_2 \cup C_5,$$

$$N_2 = \{0, 1, 2, 4, 8, 16\} = C_\infty \cup C_0.$$

Assume that  $w_1(x)$  and  $w_2(x)$  are equivalent:

$$w_2(x) = x^s w_1(x^t) \quad (s \in \mathbf{Z}_{31}, t \in \mathbf{Z}_{31}^*).$$

Since 2 is a fixing multiplier for both  $w_1(x)$  and  $w_2(x)$ ,

$$w_1(x^2) = w_1(x) \text{ and } w_2(x^2) = w_2(x).$$

Thus

$$w_2(x) = w_2(x^2) = x^{2s} w_1(x^{2t}) = x^{2s} w_1(x^t) = x^s w_2(x^t).$$

It follows that

$$P_2 = s + P_2 \text{ and } N_2 = s + N_2,$$

and obviously this implies  $s = 0$  (for the given  $P_2$  and  $N_2$ ). Thus

$$w_2(x) = w_1(x^t)$$

so that

$$P_2 = tP_1 \text{ and } N_2 = tN_1.$$

Multiplication by  $t$  maps 2-orbits to 2-orbits (of the same length, and thus  $tC_\infty = C_\infty$  and  $tC_0 = C_0$ ). It follows that  $t = t \cdot 1 \in tC_\infty = C_\infty$ , i.e.,  $t$  is a power of 2(mod31). Thus  $w_2(x) = w_1(x^t) = w_1(x)$ .

By Theorems 8.2 and 8.3 we get that for every odd  $d \geq 1$  there are two distinct equivalence classes in  $CW(31m, 16)$  with  $olp(P) = 5^2$  and  $olp(N) = 1^1 5^1$ . They are

- $\widetilde{w}_1(x) = -1 - x^m - x^{2m} + x^{3m} - x^{4m} + x^{6m} + x^{7m} - x^{8m} + x^{12m} + x^{14m} - x^{16m} + x^{17m} + x^{19m} + x^{24m} + x^{25m} + x^{28m},$
- $\widetilde{w}_2(x) = -1 - x^m - x^{2m} - x^{4m} + x^{5m} - x^{8m} + x^{9m} + x^{10m} + x^{15m} - x^{16m} + x^{18m} + x^{20m} + x^{23m} + x^{27m} + x^{29m} + x^{30m}.$

2.  $P = \{a, b, 2b, 4b, c, 2c, 4c, 8c, 16c, 32c\}; N = \{d, 2d, 4d, 8d, 16d, 32d\};$   
 $ol(a) = 1, ol(b) = 3, ol(c) = 6; ol(d) = 6.$

$P$  and  $N$  contain orbits of lengths 1, 3 and 6. By Section 5,  $n$  must satisfy the following conditions for the existence of orbits of length  $i$ , for  $i \in \{1, 3, 6\}$ . By Section 5

- $i = 1$ :  $n$  arbitrary.
- $i = 3$ :  $n$  must be divisible by 7.
- $i = 6$ : In this case, the precise restrictions on  $n$  depend on the number of different orbits of length 6 in  $P \cup N$ . We need two orbits. Hence there are two possibilities:
  - (a)  $63 \mid n$ , so there are 9 different orbits of length 6. Therefore there are  $9 \times 8 = 72$  possibilities for the choice of the two orbits of length 6 in  $P \cup N$ .
  - (b)  $21 \mid n$  but  $63 \nmid n$ , and then there are exactly two different orbits of length 6. Therefore there are two possibilities for the choice of the two (ordered) orbits of length 6 in  $P \cup N$ .

(Recall that if  $9 \mid n$  but  $63 \nmid n$  then there is only one orbit of length 6.) Hence in the present case necessarily  $21 \mid n$ .

#### Theorem 8.4

(i) For each odd  $m \geq 1$ , if  $w(x) \in CW(21m, 16)$  has (for the multiplier  $t = 2$ )

$$olp(P) = 1^1 3^1 6^1, \quad olp(N) = 6^1$$

then:

- If  $3 \nmid m$  then there exists

$$w_0(x) \in CW(21, 16) \quad \text{s. t.} \quad w(x) = w_0(x^m).$$

- If  $3|m$  then there exists

$$w'_0(x) \in CW(63, 16) \quad \text{s. t.} \quad w(x) = w'_0(x^{\frac{m}{3}}).$$

(ii) If  $w(x)$  and  $\tilde{w}(x)$  are equivalent in  $R_{21m}$  then:

- If  $3 \nmid m$  then  $w_0(x)$  and  $\tilde{w}_0(x)$  are equivalent in  $R_{21}$ .
- If  $3|m$  then  $w'_0(x)$  and  $\tilde{w}'_0(x)$  are equivalent in  $R_{63}$ .

### Proof

(i) Let  $m \geq 1$  be an odd integer and assume that  $w(x) \in CW(21m, 16)$  with the above  $olp(P)$ ,  $olp(N)$ . Then  $0 \in P$  (the unique element with orbit length equal to 1). Let  $x \in P$  be a generator of the orbit of length 3. According to Section 5

$$\exists j \in \{1, \dots, 6\} : \quad x = \frac{21mj}{7} = 3mj \quad \Rightarrow \quad m|x.$$

Let  $y \in P$  and  $z \in N$  be generators of the orbits of length 6. Therefore by the results of Section 5

$$\exists k \in \{1, \dots, 62\}, \quad 9 \nmid k \text{ and } 21 \nmid k$$

such that

$$y = \frac{21mk}{63} = \frac{mk}{3}.$$

Similarly for  $z$ . The following cases are possible:

- $3 \nmid m$ .

Here necessarily  $3|k$ . Hence  $m|y$  and similarly for  $z$ . Thus we obtain

$$m|s \quad (\forall s \in P \cup N),$$

so there is a (unique) polynomial  $w_0(x) \in R_{21}$  s.t.  $w(x) = w_0(x^m)$ . Obviously,  $w_0(x) \in CW(21, 16)$ .

- $3|m$ .

Let  $m = 3m'$ . Then  $y = m'k \Rightarrow m'|y$ . Similarly for  $z$ . Note that also  $m'|x$ .

Thus

$$m'|s \quad (\forall s \in P \cup N),$$

so there is a (unique) polynomial  $w'_0(x) \in R_{63}$  s.t.

$$w(x) = w'_0(x^{m'}) = w'_0(x^{\frac{m}{3}}).$$

Obviously,  $w'_0(x) \in CW(63, 16)$ .

(ii) Proof similar to that of Theorem 8.3(ii).

◇

By Theorem 8.2 and Theorem 8.4 we now need to find all equivalence classes in  $CW(21, 16)$  and in  $CW(63, 16)$  (with the given  $olp(P)$  and  $olp(N)$ ). Note that if  $w(x) \in CW(21, 16)$  then  $w(x^3) \in CW(63, 16)$ . The data that we have consist of

$$n = 63, \quad k = 16, \quad t = 2, \quad olp(P) = 1^1 3^1 6^1, \quad olp(N) = 6^1.$$

We will search for  $P$  and  $N$  with the help of a Pascal program. This program is very similar to the one described above in the case of  $CW(31, 16)$ . It was run, giving 8 solutions. Another Pascal program was designed to check equivalence between the polynomials obtained. It showed that every  $w(x) \in CW(63, 16)$  is equivalent to one of the following two polynomials:

$$(a) \quad w_1(x) = 1 - x^1 - x^2 - x^4 - x^8 + x^9 + x^{13} - x^{16} + x^{18} + x^{19} + x^{26} - x^{32} + x^{36} + x^{38} + x^{41} + x^{52}$$

$$(b) \quad w_2(x) = 1 - x^3 - x^6 - x^{12} + x^{15} - x^{24} + x^{27} + x^{30} - x^{33} + x^{39} + x^{45} - x^{48} + x^{51} + x^{54} + x^{57} + x^{60}$$

As in the case of  $CW(31, 16)$ , it may be easily shown that  $w_1(x)$  and  $w_2(x)$  are inequivalent.

By Theorems 8.2 and 8.4 there are two distinct equivalence classes in  $CW(63m, 31)$ , for each odd  $m \geq 1$ :

$$\bullet \quad \widetilde{w}_1(x) = 1 - x^m - x^{2m} - x^{4m} - x^{8m} + x^{9m} + x^{13m} - x^{16m} + x^{18m} + x^{19m} + x^{26m} - x^{32m} + x^{36m} + x^{38m} + x^{41m} + x^{52m},$$



- $\widetilde{w}_2(x) = 1 - x^{3m} - x^{6m} - x^{12m} + x^{15m} - x^{24m} + x^{27m} + x^{30m} - x^{33m} + x^{39m} + x^{45m} - x^{48m} + x^{51m} + x^{54m} + x^{57m} + x^{60m}.$

It easy to see that  $w_2(x)$  above satisfies

$$3 \mid s \quad (\forall s \in P \cup N),$$

and that no polynomial equivalent to  $w_1(x)$  has this property. Thus  $w'(x) := w_2(x^{\frac{1}{3}})$  is a solution in  $CW(21, 16)$ :

$$w'(x) = 1 - x^1 - x^2 - x^4 + x^5 - x^8 + x^9 + x^{10} - x^{11} + x^{13} + x^{15} - x^{16} + x^{17} + x^{18} + x^{19} + x^{20}.$$

Hence there is only one equivalence class in  $CW(21, 16)$ . This gives an equivalence class in  $CW(21m, 16)$  for each  $m \geq 1$ :

$$\widetilde{w'}(x) = 1 - x^m - x^{2m} - x^{4m} + x^{5m} - x^{8m} + x^{9m} + x^{10m} - x^{11m} + x^{13m} + x^{15m} - x^{16m} + x^{17m} + x^{18m} + x^{19m} + x^{20m}.$$

3.  $P = \{a, 2a, 4a, 8a, b, 2b, 4b, 8b, 16b, 32b\}$ ;  $N = \{c, 2c, d, 2d, 4d, 8d\}$ ;  
 $ol(a) = 4, ol(b) = 6; ol(c) = 2, ol(d) = 4.$

$P$  and  $N$  contain orbits of lengths 2, 4 and 6. By Section 5,  $n$  must satisfy the conditions for the existence of orbits of length  $i$ , for  $i \in \{2, 4, 6\}$ :

- $i = 2$ :  $n$  must be divisible by 3.
- $i = 4$ :  $n$  must be divisible by 15; recall that if  $5 \mid n$  but  $15 \nmid n$  then there is only one orbit of length 4.
- $i = 6$ : Here we need only one orbit of length 6 in  $P \cup N$ . Hence there are three possibilities:
  - (a)  $63 \mid n$ , and then there are 9 different orbits of length 6.
  - (b)  $21 \mid n$  but  $63 \nmid n$ , and then there are two different orbits of length 6.
  - (c)  $9 \mid n$  but  $63 \nmid n$ , and then there is only one orbit of length 6.

Hence in the present case necessarily either  $45 \mid n$  or  $105 \mid n$ . The proofs of the following theorems are similar to those of Theorems 8.3 and 8.4, and will be omitted.

**Theorem 8.5**

(i) For each odd  $m \geq 1$ , if  $w(x) \in CW(45m, 16)$  has (for the multiplier  $t = 2$ )

$$olp(P) = 4^1 6^1, \quad olp(N) = 2^1 4^1$$

then:

- If  $7 \nmid m$  then there exists

$$w_0(x) \in CW(45, 16) \quad \text{s. t.} \quad w(x) = w_0(x^m).$$

- If  $7|m$  then there exists

$$w'_0(x) \in CW(315, 16) \quad \text{s. t.} \quad w(x) = w'_0(x^{\frac{m}{7}}).$$

(ii) If  $w(x)$  and  $\tilde{w}(x)$  are equivalent in  $R_{45m}$  then:

- If  $7 \nmid m$  then  $w_0(x)$  and  $\tilde{w}_0(x)$  are equivalent in  $R_{45}$ .
- If  $7|m$  then  $w'_0(x)$  and  $\tilde{w}'_0(x)$  are equivalent in  $R_{315}$ .

◇

**Theorem 8.6**

(i) For each odd  $m \geq 1$ , if  $w(x) \in CW(105m, 16)$  has (for the multiplier  $t = 2$ )

$$olp(P) = 4^1 6^1, \quad olp(N) = 2^1 4^1$$

then:

- If  $3 \nmid m$  then there exists

$$w_0(x) \in CW(105, 16) \quad \text{s. t.} \quad w(x) = w_0(x^m).$$

- If  $3|m$  then there exists

$$w'_0(x) \in CW(315, 16) \quad \text{s. t.} \quad w(x) = w'_0(x^{\frac{m}{3}}).$$

(ii) If  $w(x)$  and  $\tilde{w}(x)$  are equivalent in  $R_{105m}$  then:

- If  $3 \nmid m$  then  $w_0(x)$  and  $\tilde{w}_0(x)$  are equivalent in  $R_{105}$ .
- If  $3|m$  then  $w'_0(x)$  and  $\tilde{w}'_0(x)$  are equivalent in  $R_{315}$ .

◇

By Theorems 8.2, 8.5 and 8.6 we have to search for circulant weighing only in  $CW(315, 16)$ . This search will also give all solutions in  $CW(45, 16)$  and in  $CW(105, 16)$ . The data that we have consist of

$$n = 315, \quad k = 16, \quad t = 2, \quad \text{olp}(P) = 4^1 6^1, \quad \text{olp}(N) = 2^1 4^1.$$

A Pascal program, completely analogous to the ones described in the previous cases, was written and run. No solutions were found. Hence there does not exist  $w(x) \in CW(n, 16)$  with the above data.

## 9 Summary

The following results were obtained in this paper.

- $CW(21, 16) \neq \emptyset$ . Only one equivalence class exists here (it was known before this work):

$$w_0(x) = 1 - x^1 - x^2 - x^4 + x^5 - x^8 + x^9 + x^{10} - x^{11} + x^{13} + x^{15} - x^{16} + x^{17} + x^{18} + x^{19} + x^{20}.$$

- $CW(31, 16) \neq \emptyset$ . There are two distinct equivalence classes (both were known before):

$$w_1(x) = -1 - x - x^2 + x^3 - x^4 + x^6 + x^7 - x^8 + x^{12} + x^{14} - x^{16} + x^{17} + x^{19} + x^{24} + x^{25} + x^{28},$$

$$w_2(x) = -1 - x - x^2 - x^4 + x^5 - x^8 + x^9 + x^{10} + x^{15} - x^{16} + x^{18} + x^{20} + x^{23} + x^{27} + x^{29} + x^{30}.$$

- $CW(63, 16) \neq \emptyset$ . Two distinct equivalence classes exist in this case:

$$w'_1(x) = 1 - x^1 - x^2 - x^4 - x^8 + x^9 + x^{13} - x^{16} + x^{18} + x^{19} + x^{26} - x^{32} + x^{36} + x^{38} + x^{41} + x^{52},$$

[a new class which wasn't known before this work]

$$w'_2(x) = 1 - x^3 - x^6 - x^{12} + x^{15} - x^{24} + x^{27} + x^{30} - x^{33} + x^{39} + x^{45} - x^{48} + x^{51} + x^{54} + x^{57} + x^{60}.$$

[an old class:  $w'_2(x) = w_0(x^3)$  with  $w_0(x) \in CW(21, 16)$  above]

- $CW(n, 16) \neq \emptyset$ , for odd  $n$ , iff either  $21|n$  or  $31|n$ . In each case, representatives for all possible equivalence classes are obtained by replacing  $x$  by  $x^m$  in one of the above polynomials, for a suitable integral value of  $m$  ( $\frac{n}{21}$ ,  $\frac{n}{31}$ , or  $\frac{n}{63}$ ). The number of equivalence classes is at most 4. More specifically:

If  $31|n$  and  $63|n$  then there are 4 classes.

If  $31|n$  and  $21|n$  but  $63 \nmid n$  then there are 3 classes.

If  $31|n$  but  $21 \nmid n$  then there are 2 classes.

If  $31 \nmid n$  but  $63|n$  then there are 2 classes.

If  $31 \nmid n$  and  $63 \nmid n$  but  $21|n$  then there is one class.

Otherwise ( $31 \nmid n$  and  $21 \nmid n$ ) - there are no classes.

## References

- [1] R.M. Adin, M. Muzychuk and Y. Strassler, Circulant weighing matrices of prime order via symmetric polynomials, in preparation.
- [2] K.T. Arasu, J.F. Dillon, D. Jungnickel and A. Pott, The solution of the Waterloo problem, J. of Combinatorial Theory (Series A) 71, 316-331, 1995.
- [3] K.T. Arasu and J. Seberry, Circulant weighing designs, J. of Combinatorial Designs 4, 439-447, 1996.
- [4] K.T. Arasu and J. Seberry, On circulant weighing matrices, preprint, 1998.
- [5] K.S. Banerjee, Weighing Designs for Chemistry, Medicine, Economics, Operations Research, Statistics, M. Dekker, New York, 1975.
- [6] R. Craigen, Constructions for Orthogonal Matrices, Ph.D. Thesis, The University of Waterloo, Ontario, Canada, 1991.
- [7] P. Eades, Circulant  $(v, k, \mu)$  designs, Lecture Notes in Mathematics No. 829, 83-93, Springer-Verlag, Berlin-Heidelberg, 1980.
- [8] P. Eades, R.M. Hain, On circulant weighing matrices, Ars Combinatoria 2, 265-284, 1976.
- [9] A.V. Geramita, J.M. Geramita, J. Seberry-Wallis, Orthogonal designs, J. Lin. Mult. Algebra 3, 281-306, 1975.
- [10] A.V. Geramita, J. Seberry. Orthogonal Designs (Quadratic Forms and Hadamard Matrices), Marcel Dekker, New York, 1979.

- [11] R. Hain, Circulant Weighing Matrices, M.A. Thesis, Australian National University, 1977.
- [12] E.L. Hall, Computer Image Processing and Recognition, Academic Press, New York, 1979.
- [13] M. Hall, Combinatorial Theory, 2nd Ed., Wiley-Interscience, New York, 1986.
- [14] M. Harmit and N.J.A. Sloan, Hadamard Transform Optics, Academic Press, New York, 1979.
- [15] D. Jungnickel, Difference sets, in: Jeffrey H. Dinitz and Douglas R. Stinton (editors), Contemporary Design Theory: A Collection of Surveys, John Wiley & Sons, 1992.
- [16] G.J. Koehler, A proof of the Vose-Liepins conjecture, Annals of Mathematics and Artificial Intelligence 10, 409-422, 1994.
- [17] E.S. Lander, Symmetric Designs: An Algebraic Approach, Cambridge University Press, 1983.
- [18] R.L. McFarland, On Multipliers of Abelian Difference Sets, Ph.D. Thesis, Ohio State University, 1980.
- [19] M. Muzychuk, Difference Sets with  $n = 2p^m$ , J. Algebraic Combinatorics 7, 77-89, 1998.
- [20] J. Seberry-Wallis and A.L. Whiteman, Some results on weighing matrices, Bull. Austral. Math. Soc. 12, 433-447, 1975.
- [21] J. Seberry and K. Wehrhahn, A class of codes generated by circulant weighing matrices, in: D.H. Holton and J. Seberry (editors), Proceedings of the International Conference on Combinatorial Mathematics, Canberra, August 16-27, 1977, 282-289, Springer, Berlin, 1978.
- [22] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, in: Jeffrey H. Dinitz and Douglas R. Stinton (editors), Contemporary Design Theory: A Collection of Surveys, John Wiley & Sons, 431-554, 1992.
- [23] R.G. Stanton and R.C. Mullin. On existence of a class of circulant balanced weighing matrices, SIAM J. Appl. Math. 30, 98-102, 1976.

- [24] Y. Strassler, In Search for Circulant Weighing Matrices, M.Sc. Thesis, Bar-Ilan University, 1983.
- [25] Y. Strassler, Circulant weighing matrices of prime order and weight 9 having a multiplier, manuscript.
- [26] Y. Strassler, New circulant weighing matrices of prime order in  $CW(31, 16)$ ,  $CW(71, 25)$ ,  $CW(127, 64)$ , Proceedings of the Bose Conference, J. qqStatistical Planning and Inference 73, 317-330, 1998.
- [27] Y. Strassler, The Classification of Circulant Weighing Matrices of Weight 9, Ph.D. Thesis, Bar-Ilan University, 1998.